UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA

COUPONCABIN LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	CAUSE NO.: 2:14-CV-39-TLS
	)	
SAVINGS.COM, INC., *et al.*,	)	
	)	
Defendants.	)	

OPINION AND ORDER

This matter is before the Court on a Motion to Dismiss or, in the Alternative, a Motion for a More Definite Statement [ECF No. 65] filed by the Defendants Savings.com, Inc., Linfield Media, LLC, Cox Target Media, Inc., and Sazze, Inc. d/b/a DealsPlus, on January 15, 2016. For the reasons stated in this Opinion and Order, the Court grants in part and denies in part the Defendants' Motion.

BACKGROUND

On February 7, 2014, the Plaintiff, CouponCabin LLC, filed a Complaint [ECF No. 1] against ten unnamed defendants (Does 1–10) [ECF No. 1]; and on November 2, 2015, it filed an Amended Complaint [ECF No. 28] adding the following Defendants: Savings.com, Inc., Cox Target Media, Inc., Linfield Media, LLC, Internet Brands, Inc., and Sazze, Inc. d/b/a DealsPlus. According to the Amended Complaint, the Plaintiff is a "leading provider of online, printable and grocery coupons for more than 3,000 retailers and merchants, and provides more than 20,000 active and genuine coupons, coupon codes, discount offers or deals, and/or links to same . . . through its website . . . [which] is available at no cost to the general public." (Am. Compl. ¶¶ 1, 27.)

In 2013, the Plaintiff launched an investigation in response to "a marked increase in the amount of its unique content appearing on a number of competing websites." (*Id.* at ¶ 3.) The investigation allegedly uncovered the existence of so-called "scraping programs," that were "systematically acquiring data from the [Plaintiff's] website." (*Id.* at ¶¶ 3–4 (describing "scraping programs" as "computer programs that operate to electronically copy, retrieve or otherwise acquire data and information from the websites of others with little or no human interaction.").) The Plaintiff also alleges that the investigation uncovered evidence of "manual scraping," described as "unauthorized and systematic copying, downloading, saving or other misappropriation of . . . website data by human agents." (*Id.* at ¶ 4.)

The Plaintiff claims that, since at least 2013, the Defendants have either manually scraped or employed scraping programs "in order to download, copy and/or record, and/or enable the republishing of . . . data from the [Plaintiff's] website." (*Id.* at ¶ 5.) Such practices allegedly violate the Plaintiff's Terms and Conditions, which appear on the Plaintiff's website and prohibit the "systematic retrieval (including by use or data mining, robots, or other extraction tools) of data or other content from the [Plaintiff's] website." (*Id.* (quoting Ex. A., Pl.'s Terms and Conditions).)

As a result of the investigation, the Plaintiff hired a third-party security provider to "implement[] technological safeguards and barriers" (*Id.* at ¶ 34), which included "block[ing] the access of all traffic, including legitimate users, emanating from certain cloud computing providers and internet service providers identified as being used particularly heavily by the Defendants to conduct scraping activities." (*Id.* at ¶ 35). The Plaintiff also "communicated with each of the Defendants, other than Linfield Media, LLC, to demand that they cease and desist

their data scraping, misappropriation of Coupon Content or data from the [Plaintiff's] website." (*Id.* at ¶ 74.) However, according to the Plaintiff, "the Defendants knowingly and intentionally circumvented [the Plaintiff's] security measures in order to continue their data scraping activities." (*Id.* at ¶ 40.)

The Plaintiff asserts state and federal claims against the Defendants, including: (1) a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*; (2) a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*; (3) breach of contract; (4) trespass; and (5) tortious interference. On January 15, 2016, Defendants Savings.com, Inc., Linfield Media, LLC, Cox Target Media, Inc., and Sazze, Inc. d/b/a DealsPlus (collectively, "Defendants") filed a Motion to Dismiss or, in the Alternative, a Motion for a More Definite Statement [ECF No. 65], along with an accompanying Memorandum in Support [ECF No. 66] and exhibit (i.e., screenshots of the Plaintiff's website) [ECF No. 66-1], arguing that the Plaintiff's Amended Complaint should be dismissed in its entirety for failure to state a claim;[1] or alternatively, that the Plaintiff must provide a more definite statement under Federal Rule of Civil Procedure 12(e). On February 8, 2016, the Plaintiff filed a Response [ECF No. 69], and on March 3, 2016, the Defendants filed a Reply [ECF No. 78].[2] The Motion is now fully briefed and

[1]The Defendants do not challenge the Plaintiff's state claims for trespass and tortious interference on the basis of Rule 12(b)(6); but instead, on the basis that a district court may decline to exercise supplemental jurisdiction if "the district court has dismissed all claims over which it has original jurisdiction." 28 U.S.C. § 1367(c)(3); *see also Groce v. Eli Lilly & Co.*, 193 F.3d 496, 501 (7th Cir. 1999) (noting that established law of this circuit is that the "usual practice" is to dismiss without prejudice state supplemental claims whenever all federal claims have been dismissed before trial).

[2]On April 13, 2016, the Defendants filed a Notice of Recent Decision [ECF No. 79], indicating that the Seventh Circuit affirmed *Sgouros v. TransUnion Corp*, No. 14 C 1850, 2015 WL 507584 (N.D. Ill. Feb. 5, 2015), which the Defendants cite in their Memorandum. *See Sgouros v. TransUnion Corp.*, 817 F.3d 1029 (7th Cir. 2016).

ripe for ruling.

DISCUSSION

I. Rule 12(b)(6) Motion to Dismiss

A motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) tests the sufficiency of the complaint and not the merits of the suit. *Gibson v. City of Chi.*, 910 F.2d 1510, 1520 (7th Cir. 1990). The court presumes all well-pleaded allegations to be true, views them in the light most favorable to the plaintiff, and accepts as true all reasonable inferences to be drawn from the allegations. *Whirlpool Fin. Corp. v. GN Holdings, Inc.*, 67 F.3d 605, 608 (7th Cir. 1995).

The Supreme Court has articulated the following standard regarding factual allegations that are required to survive dismissal:

> While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact).

Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007) (internal quotation marks, ellipsis, citations, and footnote omitted). A complaint must contain sufficient factual matter to "state a claim to relief that is plausible on its face." *Id.* at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556).

Additionally, pursuant to Rule 12(d), a motion to dismiss for failure to state a claim that includes matters outside of the pleadings must be treated as a motion for summary judgment under Rule 56. *See, e.g.*, *Levenstein v. Salafsky*, 164 F.3d 345, 347 (7th Cir. 1998). However, a court is not required to convert a motion to dismiss to a motion for summary judgment if the additional documents it considers are referenced in the complaint and are central to the claim. *Citadel Grp. v. Wash. Reg'l Med. Ctr.*, 692 F.3d 580, 591 (7th Cir. 2012). "Such documents may permit the court to determine that the plaintiff is not entitled to judgment." *Reger Dev., LLC v. Nat'l City Bank*, 592 F.3d 759, 764 (7th Cir. 2010) (citing *Hecker v. Deere & Co.*, 556 F.3d 575, 588 (7th Cir. 2009)). Because the Plaintiff's website is referenced in the Complaint and is central to the Plaintiff's claim, the Court will consider the Defendants' exhibit [ECF No. 66-1] in conjunction with the pleadings.

A. Computer Fraud and Abuse Act (CFAA) Claim (Count I)

The CFAA imposes both civil and criminal liability for the unauthorized access of electronic data. 18 U.S.C. § 1030(a)(1–7). Of relevance here, an individual violates the CFAA if he "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains . . . information from any protected computer." § 1030(a)(2); *see Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 766 (N.D. Ill. 2009) ("The elements of a section 1030(a)(2) violation . . . include (1) intentional access of a computer, (2) without or in excess of authorization, (3) whereby the defendant obtains information from the protected computer."). The CFAA does not define "without authorization"; although it does define "exceeds authorized access," as "to access a computer with authorization and to use such access to obtain or alter

information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

In seeking dismissal, the Defendants note that liability under § 1030(a)(2) is triggered by the unauthorized *access* of electronic data—not by the unauthorized *use* of such data. Def.'s Br. 7–9 (citing *Bittman v. Fox*, 107 F. Supp. 3d 896, 900–901 (N.D. Ill. 2015) ("The statutory purpose of the CFAA is to punish trespassers and hackers."), *CollegeSource, Inc. v. AcademyOne, Inc.*, Civil Action No. 10-3542, 2012 WL 5269213, at *14 (E.D. Pa. Oct. 25, 2012) ("The CFAA protects against unauthorized access rather than unauthorized use"), and *Koch Indus., Inc. v. Does*, No. 2:10CV1275DAK, 2011 WL 1775765, at *8 (D. Utah May 9, 2011) (noting that "[a] majority of courts have concluded" that claims of unauthorized use "lie outside the scope of the CFAA."). According to the Defendants, because the Plaintiff alleges the "scraping" of electronic data that is publicly accessible, it is attempting to hold the Defendants liable for the unauthorized *use* of electronic data.

The Plaintiff counters, in essence, that liability turns on the Court's interpretation of the term "without authorization"—and in particular, whether a party acts "without authorization" when permission to access a public website has been affirmatively restricted or revoked. Recall that in the Amended Complaint, the Plaintiff claims that it undertook affirmative steps to restrict and/or revoke the Defendants' access to its website by "block[ing] the access of all traffic, including legitimate users, emanating from certain cloud computing providers and internet service providers identified as being used particularly heavily by the Defendants to conduct scraping activities" and by "communicat[ing] with each of the Defendants, other than Linfield Media, LLC, to demand that they cease and desist their data scraping, misappropriation of

Coupon Content or data from the [Plaintiff's] website." (Am Compl. ¶¶ 35, 74); *see also id.* at ¶ 40 (alleging that "[s]ometime after [the Plaintiff] blocked the Defendants from accessing the [Plaintiff's] website, the Defendants knowingly and intentionally circumvented [the Plaintiff's] security measures in order to continue their data scraping activities.").

Because the CFAA does not define "authorization," the Court must give the term its "'ordinary and plain meaning.'" *United States v. Patel*, 778 F.3d 607, 613 (7th Cir. 2015) (quoting *Sanders v. Jackson*, 209 F.3d 998, 1000 (7th Cir. 2000) (noting that "[w]e frequently look to dictionaries to determine the plain meaning of words, and in particular we look at how a phrase was defined at the time the statute was drafted and enacted.")). The Oxford English Dictionary defines "Authorization" as "[t]he action of authorizing a person or thing" or "formal permission or approval." Authorization, oed.com, http://www.oed.com/view/Entry/13351?redirectedFrom=authorization#eid (last visited June 7, 2016). Moreover, the term, "authorize," ordinarily means "to give official permission for or formal approval to (an action, undertaking, etc.)" or "to approve, sanction." Authorize, oed.com, http://www.oed.com/view/Entry/13352?redirectedFrom=authorize#eid (last visited June 7, 2016). Therefore, based on the ordinary and plain meaning of "authorization," to act "without authorization" is to act without formal permission or approval.

A review of case law shows that several district courts have adopted a similar interpretation of "without authorization" when confronting nearly identical facts. For example, in *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013), a defendant accessed the plaintiff's public website even after the plaintiff sent cease-and-desist letters and blocked the defendant's IP addresses. *Id.* at 1180–81. In finding that the defendant acted "without

authorization" under the CFAA, the court explained that although the plaintiff "gave the world permission (i.e., 'authorization') to access the public information on its public website . . . it rescinded that permission for [the defendant]. Further access by [the defendant] after that rescission was 'without authorization.'" *Id.* at 1184; *see also Facebook, Inc. v. Grunin*, 77 F. Supp. 3d 965, 973 (N.D. Cal. 2015) (finding that a defendant acted "without authorization" under the CFAA when he continued to access Facebook's site, even after Facebook "implemented a complete access restriction by sending [the defendant] two cease-and-desist letters and by taking technical measures to block his access."); *Sw. Airlines v. Farechase*, 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004) (finding that a plaintiff plausibly alleged a CFAA claim when Southwest "directly informed" the defendant that its scraping activity violated the Use Agreement on Southwest's website, which was "accessible from all pages on the website," as well as via "direct repeated warnings and requests to stop scraping.") (internal quotation marks and citation omitted); *cf QVC, Inc. v. Resultly, LLC*, —F. Supp. 3d—, 2016 WL 521197, at *13 (E.D. Pa. Feb. 10. 2016) (noting that, in determining whether the defendant acted "without authorization," the "relevant question is not whether [the defendant] was granted permission to access the information on QVC.com, but whether that authorization was ever rescinded or limited in a way that would put [the defendant] on notice that it was not authorized to access information it was otherwise entitled to access.").

Guidance as to the meaning of "without authorization" is also found in CFAA cases involving employer-employee relationships. Notably, in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit found that an employee acted "without authorization" despite the absence of any "hacking" or other techniques aimed at penetrating a

secure computer or network on the part of the employee. *Id.* at 420 (finding that even though an employee was authorized to use his employer's laptop in a general sense, the defendant's "authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit . . . he resolved to destroy files that incriminated himself and other files that were the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.") (citation omitted); *cf. LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133–34 (9th Cir. 2009) ("[A] person uses a computer 'without authorization' . . . when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access someone's computer and the defendant uses the computer anyway.")

Thus, given the "ordinary and plain meaning" of "authorization," coupled with the case law described above, the Court is persuaded that CFAA liability may exist in certain situations where a party's authorization to access electronic data—including publicly accessible electronic data—has been affirmatively rescinded or revoked. By alleging that the Defendants knowingly and intentionally circumvented the Plaintiff's security measures after the Plaintiff blocked access from certain cloud computing/internet service providers and communicated with the Defendants by demanding that they cease and desist scraping-related activities, the Plaintiff has pled enough facts to survive dismissal. The Motion to Dismiss, as it relates to Count I, is denied.

B. Digital Millennium Copyright Act (DMCA) Claim (Count II)

Next, the Plaintiff alleges that the Defendants violated the DMCA, 17 U.S.C. § 1201 *et seq.*, which provides both civil and criminal liability "'to protect [copyright owners'] works from

piracy behind digital walls such as encryption codes or password protections.'" *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 458 (2007) (quoting *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001)). Of relevance here, the DMCA contains three provisions aimed at combating the circumvention of technical measures implemented by copyright owners: (1) § 1201(a)(1)(A), which prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under [the Copyright Act]"; (2) § 1201(a)(2), which prohibits trafficking in technology that circumvents a technological measure that "effectively controls access" to a copyrighted work; and (3) § 1201(b)(1), which prohibits trafficking in technology that circumvents a technological measure that "effectively protects" a copyright owner's right.

Based on the briefing, the Plaintiff appears to be alleging a DMCA claim under sections 1201(a)(1)(A) and 1201(a)(2). In *Chamberlain Group v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004), the Federal Circuit found that a plaintiff alleging a violation of § 1201(a) must prove the following:

> (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (I) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure. A plaintiff incapable of establishing any one of elements (1) through (5) will have failed to prove a prima facie case. A plaintiff capable of proving elements (1) through (5) need prove only one of (6)(I), (ii), or (iii) to shift the burden back to the defendant. At that point, the various affirmative defenses enumerated throughout § 1201 become relevant.

381 F.3d 1178, 1203 (italics omitted) (on appeal from the Northern District of Illinois and applying Seventh Circuit law); *see also Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005) (same). To "'circumvent a technological

measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." § 1201(a)(3)(A). Further, "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." § 1201(a)(3)(B).

Notably, in *Chamberlain*, a violation of § 1201(a) requires a plaintiff to show that "the access resulting from the circumvention of the technological measure [was] in a manner that 'infringes or facilitates infringing a right protected by the Copyright Act.'" *Nordstrom Consulting, Inc. v. M&S Techs., Inc.*, No. 06 C 3234, 2008 WL 623660, at *8 (N.D. Ill. 2008) (quoting *Chamberlain*, 381 F.3d at 1203). Thus, "[a] copyright owner seeking to impose liability on an accused circumventor must demonstrate a reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization." *Chamberlain*, 381 F.3d at 1204. *Chamberlain's* so-called "infringement nexus requirement" has been adopted by several courts, including district courts in this Circuit. *See, e.g., Nordstrom*, 2008 WL 623660, at *8; *Agfa Monotype Corp. v. Adobe Sys.*, 404 F. Supp. 2d 1030, 1034–35 (N.D. Ill. 2005); *accord Universal City Studios*, 273 F.3d at 435 (explaining that Congress enacted the DMCA to help copyright owners protect their works from piracy); *but see MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 948–52 (9th Cir. 2010) (rejecting *Chamberlain* and finding that only an incidental relation must exist between circumvention and copyright infringement).

The Defendants urge the Court to adopt *Chamberlain*, arguing that dismissal is

appropriate because the Plaintiff fails to allege a sufficient nexus between the circumvention at issue and copyright infringement. Alternatively, the Defendants argue that the Plaintiff fails to allege facts demonstrating that a copyrighted work was "effectively controlled" by a technological measure.

Notwithstanding the potential application of *Chamberlain's* "infringement nexus requirement," dismissal is appropriate here because the Plaintiff has not pled sufficient facts to show that its copyrighted work was "effectively controlled" by a technological measure. Again, a technological measure effectively controls access to a work "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." § 1201(a)(3)(B). Although the Plaintiff alleges that it implemented "technological safeguards and barriers" to control access to its website (Am. Compl. at ¶ 34), it also alleges that the Defendants continued their scraping activity by accessing the Plaintiff's website "using a variety of servers and/or internet service providers throughout the United States and/or from outside the United States" (*id.* at ¶ 44). In other words, even after the Plaintiff's implementation of "technological safeguards and barriers," its website remains accessible to users of servers and/or internet service providers that have not been blocked by the Plaintiff's technology. *See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 547 (6th Cir. 2004) ("Just as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock . . . it does not make sense to say that [§ 1201(a)] of the DMCA applies to otherwise-readily-accessible copyrighted works."); Theresa M. Troupson, *Yes, It's Illegal to Cheat a Paywall: Access Rights and the DMCA's Anticircumvention Provision*, 90 N.Y.U. L.

Rev. 325, 339 (2015) ("[A] technological protection measure must serve as a gatekeeper for all access; after all, a locked back door can hardly be said to effectively control access to a house if its front door is wide open."). Absent allegations that a user of the Plaintiff's website is required to apply "information or a process or treatment" to gain access (e.g., by providing a password), the Court is not convinced that the DMCA covers the alleged conduct at issue.

Accordingly, Count II will be dismissed without prejudice, with leave to refile if the Plaintiff is able to successfully amend its complaint consistent with this Order within 14 days of the date of this Order. *See Foster v. DeLuca*, 545 F.3d 582, 584 (7th Cir. 2008) ("District courts routinely do not terminate a case at the same time that they grant a defendant's motion to dismiss; rather, they generally dismiss the plaintiff's complaint without prejudice and give the plaintiff at least one opportunity to amend her complaint."); *Barry Aviation Inc. v. Land O'Lakes Mun. Airport Comm'n*, 377 F.3d 682, 687 (7th Cir. 2004) (stating that the general rule is that "the district court should grant leave to amend after granting a motion to dismiss").

C. Breach of Contract Claim (Counts III)

The Plaintiff also asserts breach of contract, alleging that the Defendants violated its Terms and Conditions, which appear on its website and prohibit the "systematic retrieval (including by use or data mining, robots, or other extraction tools) of data or other content from the [Plaintiff's] website." (Am. Compl. ¶ 5 (quoting Ex. A., Pl.'s Terms and Conditions).) Users of the Plaintiff's website "signify their acceptance of the [Plaintiff's] Terms and Conditions by virtue of their access and use of the Site." (*Id.* at ¶ 28 ("The Terms and Conditions state that, '[b]y using the Site, you signify your agreement to these terms and conditions and [the

Plaintiff's] Privacy Policy.'").)

As an initial matter, because the Plaintiff's federal claims create a basis for subject matter jurisdiction pursuant to 28 U.S.C. § 1331 (federal question), the Court has jurisdiction over the Plaintiff's state claims pursuant to 28 U.S.C. § 1367 (supplemental jurisdiction). Under the familiar rule of *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938)—which is applicable to state law claims that are brought through supplemental jurisdiction, *Houben v. Telular Corp.*, 309 F.3d 1028, 1032 (7th Cir. 2012)—a federal court sitting in diversity applies the substantive law of the state in which it sits; which in this case, is the substantive law of Indiana.

"The law concerning contracts is well settled in Indiana. An offer, acceptance, plus consideration make up the basis for a contract." *Dimizio v. Romo*, 756 N.E.2d 1018, 1022 (Ind. Ct. App. 2001). "A mutual assent or a meeting of the minds on all essential elements or terms must exist in order to form a binding contract." *Homer v. Burman*, 743 N.E.2d 1144, 1146–47 (Ind. Ct. App. 2001) ("Assent to th[e] terms of a contract may be expressed by acts which manifest acceptance.") (internal quotation marks and citation omitted). But as far as the Court can tell, Indiana courts have not weighed in on the validity of so-called "browsewrap agreements," which is the type of agreement at issue here. *See Sgouros v. TransUnion Corp*, No. 14 C 1850, 2015 WL 507584, at *6 (N.D. Ill. Feb. 5, 2015) (noting that browsewrap agreements "do not require users to sign a document or click an 'accept' or 'I agree' button, so users are considered to give assent simply by using the website.") (internal quotation marks and citation omitted).[3]

[3]An alternative to a browsewrap agreement is a "clickwrap agreement," which requires an affirmative act on the part of the user to manifest assent—namely, the user's clicking of a button accompanying a statement instructing the user that their click constitutes acceptance to the terms at issue. *Sgouros*, 2015 WL 507584, at *4.

However, several district courts in this Circuit have found browsewrap agreements to be enforceable when a user has actual or constructive knowledge of the website's terms and conditions. *See, e.g., id.* at *6; *Hussein v. Coinabul, LLC*, No. 14 C 5735, 2014 WL 7261240, at *2–3 (N.D. Ill. Dec. 19, 2014); *Van Tassell v. United Mktg. Grp., LLC*, 795 F. Supp. 2d 770, 790–91 (N.D. Ill. 2011); *see also Nguyen v. Barnes & Noble*, 763 F.3d 1171, 1176 (9th Cir. 2014). Thus, "[w]hen there is no evidence that users had actual knowledge of terms at issue, the validity of a browsewrap contract hinges on whether a website provided reasonable notice of the terms of the contract, i.e., whether users could have completed their purchases without ever having notice that their purchases are bound by the terms." *Sgouros*, 2015 WL 507584, at *6 (internal quotation marks and citation omitted).

The Defendants argue that the Plaintiff has failed to allege the existence of an enforceable browsewrap agreement; namely, by failing to show that the Defendants had actual or constructive notice of the Terms and Conditions. The Defendants note that

> [t]he hyperlink directing users to Plaintiff's Terms of Use is listed below 16 other links at the bottom of every page of the CouponCabin website. And while the hyperlink's font (white) is adequately contrasted by the color of its background (grey), it is buried at the bottom of each webpage. On the homepage alone, a user must scroll through nine screen shots to arrive at the hyperlink of the Terms and Conditions. Additionally, if printing the homepage, the hyperlink appears at the end of a 14-page printout.

(Defs.' Br. 18 (internal quotation marks and citations omitted).)

After reviewing the Plaintiff's website, as presented in the Defendants' exhibit [ECF No. 66-1], the Court agrees that a user is not immediately confronted with the Plaintiff's Terms and Conditions; and therefore, a reasonable argument can be made that the Terms and Conditions fail to provide constructive notice. Nevertheless, the Court is required to view the complaint

allegations in a light most favorable to the Plaintiff, and accept as true all reasonable inferences to be drawn from the allegations. *Whirlpool*, 67 F.3d at 608. The Court is therefore reluctant to declare the browsewrap agreement's unenforceability at this early stage of the litigation—particularly in light of the Plaintiff's allegations that the Defendants "knowingly and intentionally circumvented [the Plaintiff's] security measures in order to continue their data scraping activities" (Am. Compl. ¶ 40), even after the Plaintiff communicated with the Defendants and "demand[ed] that they cease and desist their data scraping, misappropriation of Coupon Content or data from the [Plaintiff's] website" (*id.* at ¶ 74). Based on these pleadings, a determination as to whether the Defendants had sufficient notice of the Terms and Conditions is more appropriately answered at a later point in the litigation.

II. Rule 12(e) Motion for a More Definite Statement

Lastly, the Defendants move for a more definite statement pursuant to Rule 12(e). A motion for a more definite statement will be granted if a "pleading to which a responsive pleading is allowed but which is so vague or ambiguous that the party cannot reasonably prepare a response." Fed. R. Civ. P. 12(e). "[B]ecause of the availability of extensive discovery, Rule 12(e) motions are disfavored and reserved for 'the rare case' where the answering party will not be able to frame a responsive pleading. Thus, courts seldom grant these motions unless the complaint is downright unintelligible or the heightened requirements of Rule 9(b) apply." *Nikolic v. St. Catherine Hosp.*, No. 2:10 CV 406, 2011 WL 4537911, at *6 (N.D. Ind. Sept. 28, 2011) (quoting *Schaedler v. Reading Eagle Publ'n, Inc.*, 370 F.2d 795, 798 (3d Cir. 1967) and citing *Bank of Am. Leasing & Capital, LLC v. Global Grp., Inc.*, 2:10–CV–390–WCL–PRC,

2011 WL 53088, at *1 (N.D. Ind. Jan.7, 2011) (explaining that Rule 12(e) motions are disfavored, but are appropriate where the plaintiff fails to satisfy Rule 9(b)), *MacNeil Auto. Prods., Ltd. v. Cannon Auto. Ltd.*, 715 F. Supp. 2d 786, 790 (N.D. Ill. 2010) (emphasizing that motions for a more definite statement do not lie as a substitute for discovery; they should be granted only where the attacked pleading is so unintelligible that the movant cannot respond), and *Moore v. Fid. Fin. Servs., Inc.*, 869 F. Supp. 557, 559–61 (N.D. Ill. 1994) (denying a Rule 12(e) motion where discovery would allow the defendant to "easily" determine the plaintiff's contentions)).

Although the Plaintiff's claims are not subject to heightened pleading standards, the Defendants argue that the Amended Complaint is insufficient because it includes generalized allegations "without specifically articulating any actions attributable to a single defendant."[4] (Defs.' Br. 21.) For support, the Defendants cite *Parker v. Brush Wellman, Inc.*, 377 F. Supp. 2d 1290 (N.D. Ga. 2005), a class action lawsuit against multiple defendants, all of whom were involved in the manufacture and/or use of products containing beryllium, a toxic substance. *Id.* at 1292. The plaintiffs asserted that they were exposed to a respirable form of the substance; but as the court noted, their complaint included "no factual allegations regarding whether [p]laintiffs were exposed to each individual [d]efendant's beryllium-containing products, nor are there any allegations regarding the approximate times (i.e., approximate date ranges) of alleged beryllium

[4]The Defendants also criticize the Plaintiff's use of so-called "shotgun pleading," where each count incorporates by reference all preceding paragraphs and counts of the complaint, *see CustomGuide v. CareerBuilder, LLC*, 813 F. Supp. 2d 990, 1001–02 (N.D. Ill. 2011) (noting that courts discourage "shotgun pleading"); along with the Plaintiff's use of the term "on information and belief" at certain points in the pleadings, *see Maclean-Fogg v. Edge Composites, L.L.C.*, Civil Action No. 08 C 6367, 2009 WL 1010426, at *6 (N.D. Ill. Apr. 14, 2009) ("Allegations based exclusively on information and belief are insufficient unless the facts are inaccessible to the pleader, and there is a reasonable basis to suspect the facts are true.").

exposure." *Id.* at 1295.

By contrast, the Plaintiff alleges that each Defendant engaged in fairly specific conduct (i.e., manual scraping, or the employment of scraping programs to "download, copy and/or record, and/or enable the republishing of, Coupon Content and other data from [the Plaintiff's] website" (Am. Compl. ¶ 5)), and that they did so within a fairly specific time frame (i.e., "[s]ince at least early fall 2013." (*Id*.). Despite the aggregated form of the complaint allegations, the Court is not persuaded that this is one of "the rare case[s]" where the answering party will not be able to frame a responsive pleading. *See Nikolic*, 2011 WL 4537911, at *6. As noted above, absent heightened pleading standards under Rule 9(b) or unintelligible pleadings, Rule 12(e) should not be used as a substitute for discovery. The Defendants' alternative request for a More Definite Statement is denied.

CONCLUSION

For the reasons stated above, the Court GRANTS IN PART and DENIES IN PART the Defendants' Motion to Dismiss [ECF No. 65]. Count II is DISMISSED WITHOUT PREJUDICE, with leave to refile within 14 days of the date of this Order.

SO ORDERED on June 8, 2016.

s/ Theresa L. Springmann
THERESA L. SPRINGMANN
UNITED STATES DISTRICT COURT
FORT WAYNE DIVISION